

Google Message Encryption and the new HIPAA legislation



ABOUT GOOGLE SECURITY AND ARCHIVING, POWERED BY POSTINI

Google security and archiving products, powered by Postini, make your existing email system more secure, compliant and productive. Built on Google's cloud-based Software as a Service (SaaS) platform, these products block spam, phishing, malware and other intrusions before they reach your network, and provide content management, encryption, and archiving to help you meet compliance challenges. Google's hosted model offers several distinct advantages. Leveraging the "network effect" created by billions of daily email connections, Google technology detects new threats in real time and blocks them across the entire Postini services network – without requiring on-site updates. Similarly, economies of scale in storage, simple deployment and maintenance-free service drive a low total cost of ownership.

For more information, visit www.google.com/postini

Overview

The Health Insurance Portability and Accountability Act (HIPAA) has changed drastically as a result of American Recovery and Reinvestment Act (ARRA). This paper highlights those changes, how they might impact your business and what you can do to address them. The new legislation has significant ramifications, most notably in the areas of enforcement, breach notification, implication for business associates, and use of encryption. A summary of specific considerations follows.

Enforcement

Under the new legislation, organizations will be fined up to \$1.5 million dollars – a dramatic increase from the former \$25,000 – for violating the rules protecting patients' privacy. These penalties are no mere slap on the wrist: enforcement will be wide-sweeping and rigorous. State Attorneys General now have clear and explicit authority to enforce HIPAA's rules.

Breach notification

There's more than financial exposure at stake. Your organization's reputation is also at risk if the security of personal data is compromised. If this occurs, new laws require that any affected parties must be alerted and told about the compromise. The breach must also be reported to the government, and, in some cases, the media must also be informed.

The implications are obvious. If your organization has a security breach, you will be heavily fined and vulnerable to visible and negative public exposure.

Implications for business associates

A new challenge to the healthcare industry is the extension of compliance responsibility to business associates. As healthcare providers partner with other services or vendors, they take on some level of risk in regards to those partners' own adherence to HIPAA guidelines. The new provisions make compliance obligatory in a true legal sense. Coupled with increased enforcement, this requirement significantly increases the risk of exposure for and the importance of clear, proactive management of sensitive information across all healthcare business relationships.

Use of encryption

In addition, because the notification provision applies only to breaches involving unsecured information, companies should evaluate an expansion of their current encryption capabilities to protect not only against realistic breaches but also to avoid new and expensive obligations under these reporting provisions. This applies to data in motion such as email, as well as to data at rest.

The new HIPAA rules pose many challenges for the health care industry. Of primary concern is ensuring that Protected Health Information (PHI) transmitted electronically via email is secured. Email is the only viable alternative for health care information exchange. It is also inherently insecure. This means email encryption should be at the top of your HIPAA compliance checklist.

Google Message Encryption (GME), powered by Postini, resolves these issues by automatically encrypting email based on your policy definitions, helping your organization avoid the financial penalties and brand equity damage that can result from sending data via unprotected email.

How Google Message Encryption supports HIPAA compliance

Google Message Encryption lets your organization securely exchange sensitive information with patients and business associates by encrypting the content transmitted over email. This automated, policy-based encryption is easy to implement and provides a more cost-effective solution than legacy on-premise email encryption infrastructures. As with all the Google hosted solutions, GME requires no additional hardware, software, updates, or maintenance.

What Google Message Encryption provides

Google Message Encryption is a hosted, cloud-based encryption service that easily, cost-effectively encrypts email, helping your business or organization to comply with the new HIPAA regulations.

- Secure messaging with business associates and patients without any additional software, hardware, or technical training
- Automatic enforcement of organizational email encryption policies based on individuals, groups, or specific message content
- User-initiated encryption for confidential messages to any email recipient
- Auditable protection of emails containing regulated or company proprietary information
- Centrally-managed security policies and reporting

For more information on how Google Message Encryption works, download our data sheet at www.google.com/a/help/intl/en/security/pdf/message_encryption.pdf

